PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: Q64735
Dominique CHANTRAIN, et al.	
Appln. No.: 09/891,545	Group Art Unit: 2153
Confirmation No.: 1856	Examiner: Yasin M. BARQADLE
Filed: June 27, 2001	

For: A METHOD FOR ENABLING A USER ALREADY CONNECTED TO A VIRTUAL PRIVATE NETWORK TO COMMUNICATE WITH A COMMUNICATION DEVICE NOT BELONGING TO THIS VIRTUAL PRIVATE NETWORK AND CORRESPONDING NETWORK ACCESS SERVER

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with 37 C.F.R. § 41.37, Appellants submit this Appeal Brief:

I. REAL PARTY IN INTEREST

The real party in interest is Alcatel Lucent.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-13 are pending. All of claims 1-13 are rejected under 35 USC 102(e) as anticipated by U.S. Patent 6,557,037 (Provino).

IV. STATUS OF AMENDMENTS

There are no amendments submitted after the final Office action of January 26, 2006.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

As explained in paragraphs [0028]-[0032] of the substitute specification filed November 2, 2004, it is common for a Network Access Server (e.g., NAS 131 in Fig. 1) to assign the same IP address to two different users connected to different VPNs. Thus, in Fig. 1, user 111 may be connected to VPN 152 and user 112 may be connected to VPN 153, but the network access server may assign the same IP address to both. If user 111 wants to communicate with a server 161 connected to VPN 151, without user 111 giving up its connection to VPN 152, a message is sent to the server 161 which will include as a source address the IP address of the user 111. If the server 161 replies to that IP address, there is ambiguity at the NAS 131 as to which of the users 111 and 112 (both having identical IP addresses) should receive the reply from server 161.

This ambiguity is avoided by the present invention by having the NAS 131, when sending the original message to the server 161, sending it on a logical channel having an identifier which is the same as the identifier of the VPN to which the user 111 is connected. When the reply comes back from the server 161 on this logical channel, the NAS 131 knows that the reply message should be directed to a user on that VPN having the indicated IP address, i.e., to user 111.

The preamble of claim 1 sets the stage for the invention, i.e., a user (111) connected to a VPN (152) via a Network Access Server (131) that has access to plural VPNs (152 and 153), with the user wanting to communicate with a device (161) not connected to the same VPN (i.e., the "host" VPN) to which the user (111) is currently connected. The first step in the method of claim 1 is the detection of a message sent from the user (user 111 connected to host VPN 152) to

a communication device (e.g., server 161) which is not connected to the host VPN (152), while the user (111) is connected to the host VPN (152). The next step is the directing of that message to a logical channel between the Network Access Server (e.g., NAS 131) and the communication device, with the logical channel having a logical channel identifier which is also the identifier of the host VPN to which the user is connected (see paragraphs [0033]-[0035] at page 10 of the substitute specification).

Independent claim 8 is directed to a Network Access Server (e.g., 131 in Fig. 1, or 20 in Fig. 2) for enabling a communication between a user (111) and a communication device (161), said user being registered in said Network Access Server as already connected to a host Virtual Private Network (152), said communication device (161) being outside of said host Virtual Private Network, said Network Access Server (20) being able to access to a database (24 in Fig. 2, paragraph [0039]) associating an identifier of said user to an identifier of said host Virtual Private Network, said Network Access Server comprising: means (21 in Fig. 2, paragraph [0040][1]) for detecting a message being sent from said user to said communication device while said user is currently connected to said host Virtual Private Network; and means (22 in Fig. 2) for sending said message on a logical channel between said Network Access Server and said communication device, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected (see, paragraph [0042]).

[1] Paragraph [0040] includes a typographical error and should refer to "first interface 201."

Independent claim 9 recites a Network Access Server (131 in Fig. 1, or 20 in Fig. 2) for identifying a user (e.g., 111), from a plurality of users (111 and 112), to which a message sent by a communication device (161) and received at said Network Access Server (20), said user (111) being already connected over said Network Access Server to a Virtual Private Network (152) not included in said communication device, said Network Access Server (20) being able to access to a database (24 in Fig. 2, paragraph [0039]) associating an identifier of said user to an identifier of said Virtual Private Network (152) to which said user is already connected, said Network Access Server comprising: a logical channel controller (22 in Fig. 2) for determining a logical channel identifier of one logical channel on which said message is received at said Network Access server (see, paragraph [0043]), wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected; and means (also 22 in Fig. 2, paragraph [0044]) for identifying the user to which said message is destined, according to said logical channel identifier and said user identifier in said database.

Independent claim 10 recites a Network Access Server (131 in Fig. 1, or 20 in Fig. 2) for enabling a communication between a user (111) and a communication device (161), said user being registered in said Network Access Server (131 or 20) as already connected to a host Virtual Private Network (152), said communication device (161) being outside of said host Virtual Private Network (152), said Network Access Server (20) being able to access to a database (24, paragraph [0039]) associating an identifier of said user to an identifier of said host Virtual Private Network, said Network Access Server comprising a forwarding engine (21,

paragraph [0040][2])) for detecting messages being sent from said user to said communication device while said user is currently connected to said host Virtual Private Network and for sending said messages originating from said user and destined to said communication device on a logical channel between said Network Access Server and said communication device, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected (paragraph [0042]).

Independent claim 12 recites a Network Access Server (131 or 20) for identifying a user (111), from a plurality of users (111 and 112), to which a message sent by a communication device (161) and received at said Network Access Server, said user (111) being already connected over said Network Access Server to a Virtual Private Network (152) not included in said communication device, said Network Access Server being able to access to a database (24, paragraph [0039]) associating an identifier of said user to an identifier of said Virtual Private Network to which said user is already connected, said Network Access Server comprising: a logical channel controller (22) for determining a logical channel identifier of one logical channel on which said message is received at said Network Access server(paragraph [0043]), wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected; and a database searcher (also 22 in Fig. 2, paragraph [0044] for identifying the user to which said message is destined, according to said logical channel identifier and said user identifier in said database.

[2] Paragraph [0040] includes a typographical error and should refer to "first interface 201."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-13 are anticipated by U.S. Patent 6,557,037 (Provino).

VII. ARGUMENT

The central concept of the present invention is that a Network Access Server (NAS) 131 in Fig. 1 serving plural users 111 and 112 each connected to a different VPN (e.g., 152 and 153 in Fig. 1), may assign the same IP address to each of the users, and when the NAS 131 sends a message from a user to a destination outside of the VPN to which that user is connected, it can continue to use the IP address of the sender as the return address, but it can set up a logical channel that is uniquely associated with the VPN to which the sender is connected. At the receive end, the logical channel identifier of the logical channel may have no particular significance. But when the receive end sends a reply to the IP address indicated as the source of the original message, it will be directed back on the same logical channel to NAS 131, and NAS 131 will be able to uniquely identify the user 111 from the combination of the IP address and the VPN associated with the logical channel.

The only rejection is for anticipation of all claims by Provino. Provino teaches a plurality of users (12(1) to 12(M)) served by a network access server (ISP 11), and discusses how one of these users 12(m) can communicate with a device within VPN 15 by sending to the firewall 30 a network address request message, the firewall 30 forwards the request to a name server 32, the name server replies to the firewall with the network address, and the firewall 30 returns this network address to the user 12(m) for use in subsequent communications. After that, the uses the supplied network address and communicates with the device via a "secure tunnel."

In his rejection, the examiner considers one of the users 12(m) to be connected to VPN 15 via ISP 11, and considers such a user to correspond to the user recited in claim 1. The

examiner then describes a situation where this user communicates with a device outside of the VPN 15. For purposes of this appeal it can be accepted that there will be an occasion on which one of the users 12(m) will communicate with a device along the paths labeled as "TO/FROM ACCESSED DEVICES" in Fig. 1. But in order for there to be anticipation, there must be a teaching in Provino that such a user is maintaining its connection to the VPN 15 while at the same time communicating with one of these other devices. There is no such discussion in Provino.

The next problem with the position of the examiner is that in attempting to find support in Provino for the claimed steps of detecting and directing, the examiner focuses exclusively on the use of the "secure tunnel." But the secure tunnel is only used for communication between a user connected to the VPN and devices inside of the VPN. This secure tunnel is what makes a Virtual Private Network "private". A commonly accepted definition of a Virtual Private Network is a data network that uses the public telecommunications infrastructure, but maintains privacy through the use of a tunneling protocol and security procedures. Thus, communications using the secure tunnel are communications between a user connected to the VPN and devices within the VPN. But claim 1 is directed to communications between a user connected to the VPN and a device outside of the VPN. There is no suggestion anywhere in Provino that communications of this sort would use a secure tunnel, so all of the discussion about secure tunnel communications is not relevant.

Still further, even if one ignores the problem that there is no teaching in Provino of a user maintaining its connection to VPN at the same time it is communicating with a device outside

the VPN, and ignoring the fact that the only described use for the secure tunnel in Provino is to allow users connected to the VPN to communicate securely with devices inside the VPN, there is also the problem that even in the secure tunnel communications there is no suggestion that the ISP 11, which the examiner equates with the claimed network access server, will establish a logical channel to such other external device, and will use a logical channel identifier an identifier of the VPN 15.

Independent claims 8-10 and 12 include essentially the same limitations that distinguish claim 1 over Provino.

In summary, a secure tunnel does not require the use of a logical channel which has an identifier which is the same as the identifier of the VPN to which the sending user is connected. There are other ways that secure communications could be managed. Further, and importantly, secure tunnel communications are only used between a user and the VPN to which the user is connected. So the secure tunnel communications in Provino cannot possibly correspond to the claimed communication between a user connected to the VPN and a device outside of the VPN.

Accordingly, it is respectfully submitted that the rejection of the examiner be reversed.

Respectfully submitted,

/DJCushing/
David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: March 21, 2007

CLAIMS APPENDIX

CLAIMS 1-13 ON APPEAL:

1. A method for enabling a user registered in an Network Access Server as already connected to a host Virtual Private Network to communicate with at least one communication device outside of said host Virtual Private Network, said Network Access Server having access over a data communication network to said communication device and to a plurality of Virtual Private Networks including said host Virtual Private Network, wherein said method comprises:

detecting a message being sent from said user to said communication device while said user is currently connected to said host Virtual Private Network; and

directing said message to a logical channel between said Network Access Server and said communication device, wherein said logical channel has, as a logical channel identifier, an identifier of said host Virtual Private Network to which said user is currently connected.

2. The method according to claim 1, wherein said method further comprises:

detecting, at said Network Access Server, the message being sent from said user to said communication device; and

forwarding said message from said Network Access Server to said communication device over said logical channel identified by the identifier of said host Virtual Private Network.

3. The method according to claim 1, wherein said method further comprises:

detecting a message from said communication device being received at said Network Access Server on the logical channel having, as a logical channel identifier, the identifier of said host Virtual Private Network, said message containing a user destination address;

determining a user registered in said Network Access Server as already connected to said host Virtual Private Network and corresponding to said destination address; and

forwarding said message from said Network Access Server to said user.

4. The method according to claim 1, wherein said messages belonging to the communication between said user and said communication device are encapsulated in data packets, said data packets comprising a field containing said identifier of said host Virtual Private Network or an indication derived from said identifier.

5. The method according to claim 4, wherein said messages belonging to the communication between said user and said communication device are sent over a tunnel, wherein said tunnel has, as a tunnel identifier, said identifier of said host Virtual Private Network.

6. The method according to claim 1, wherein said messages contain IP packets comprising an IP address of said user.

7. The method according to claim 1, wherein said communication device is a server belonging to a local Virtual Private Network associated to said Network Access Server and different from said host Virtual Private Network.

8. A Network Access Server for enabling a communication between a user and a communication device, said user being registered in said Network Access Server as already connected to a host Virtual Private Network, said communication device being outside of said host Virtual Private Network, said Network Access Server being able to access to a database associating an identifier of said user to an identifier of said host Virtual Private Network, said Network Access Server comprising:

means for detecting a message being sent from said user to said communication device while said user is currently connected to said host Virtual Private Network; and

means for sending said message on a logical channel between said Network Access Server and said communication device, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected.

9. A Network Access Server for identifying a user, from a plurality of users, to which a message sent by a communication device and received at said Network Access Server, said user being already connected over said Network Access Server to a Virtual Private Network not included in said communication device, said Network Access Server being able to access to a

database associating an identifier of said user to an identifier of said Virtual Private Network to which said user is already connected, said Network Access Server comprising:

a logical channel controller for determining a logical channel identifier of one logical channel on which said message is received at said Network Access server, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected; and

means for identifying the user to which said message is destined, according to said logical channel identifier and said user identifier in said database.

10. A Network Access Server for enabling a communication between a user and a communication device, said user being registered in said Network Access Server as already connected to a host Virtual Private Network, said communication device being outside of said host Virtual Private Network, said Network Access Server being able to access to a database associating an identifier of said user to an identifier of said host Virtual Private Network, said Network Access Server comprising a forwarding engine for detecting messages being sent from said user to said communication device while said user is currently connected to said host Virtual Private Network and for sending said messages originating from said user and destined to said communication device on a logical channel between said Network Access Server and said communication device, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected.

11. The Network Access Server according to claim 10, further comprising a logical channel controller that directs the message on the logical channel between said Network Access Server and said communication device.

12. A Network Access Server for identifying a user, from a plurality of users, to which a message sent by a communication device and received at said Network Access Server, said user being already connected over said Network Access Server to a Virtual Private Network not included in said communication device, said Network Access Server being able to access to a database associating an identifier of said user to an identifier of said Virtual Private Network to which said user is already connected, said Network Access Server comprising:

a logical channel controller for determining a logical channel identifier of one logical channel on which said message is received at said Network Access server, wherein said logical channel has, as a logical channel identifier, said identifier of said host Virtual Private Network to which said user is currently connected; and

a database searcher for identifying the user to which said message is destined, according to said logical channel identifier and said user identifier in said database.

13. The Network Access Server according to claim 12, further comprising a forwarding engine that forwards said message from said logical controller to said user after said user has been identified.

EVIDENCE APPENDIX:

There are was no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellant in the appeal.

RELATED PROCEEDINGS APPENDIX

There are no decisions rendered by a court or the Board in any proceeding identified above in Section II pursuant to 37 C.F.R. § 41.37(c)(1)(ii).

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Dominique CHANTRAIN, et al.

Docket No: Q64735

Appln. No.: 09/891,545

Group Art Unit: 2153

Confirmation No.: 1856

Examiner: Yasin M. BARQADLE

Filed: June 27, 2001

For: A METHOD FOR ENABLING A USER ALREADY CONNECTED TO A VIRTUAL PRIVATE NETWORK TO COMMUNICATE WITH A COMMUNICATION DEVICE NOT BELONGING TO THIS VIRTUAL PRIVATE NETWORK AND CORRESPONDING NETWORK ACCESS SERVER

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief. The statutory fee of $500.00 is being authorized through the Electronic Filing System (EFS).

Respectfully submitted,

/DJCushing/
David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: March 21, 2007